Radio Resource Management

Radio Resource Management について

Radio Resource Management（RRM）ソフトウェアはdeviceに組み込まれており、ワイヤレス ネットワークのリアルタイムでの無線周波数（RF）管理を一貫して行えるようにする組み込みの RF エンジニアとして機能します。RRM を使用すると、devicesは次の情報について、アソシエートされている Lightweight アクセス ポイントを継続的に監視できます。

- トラフィックの負荷：トラフィックの送受信に使用される帯域幅の合計量。これにより、無線 LAN 管理者は、ネットワークの拡大状況を追跡し、クライアントの需要を見越して計画を立てることができます。
- 干渉：他の 802.11 発信元から送られてくるトラフィック量。
- ノイズ：現在割り当てられているチャネルに干渉している 802.11 以外のトラフィック量。
- カバレッジ：接続されているすべてのクライアントの受信信号強度インジケータ（RSSI）と信号対雑音比（SNR）。
- その他：近くにあるアクセス ポイントの数。

RRM は次の機能を実行します。

- 無線リソースの監視
- 電力制御の送信
- チャネルの動的割り当て
- カバレッジ ホールの検出と修正

- RF グループ化

（注） AP が DCA チャネルのリストにないスタティック チャネルで動作している場合、RRM のグループ化は行われません。ネイバー探索プロトコル（NDP）は DCA チャネルでのみ送信されます。したがって、無線が DCA 以外のチャネルで動作している場合は、チャネルで NDP を受信しません。

無線リソースの監視

RRM は、ネットワークに追加された新しいdevicesやLightweightアクセス ポイントを自動的に検出して設定します。その後、アソシエートされている近くの Lightweight アクセス ポイントを自動的に調整して、カバレッジとキャパシティを最適化します。

Lightweight アクセス ポイントでは、使用国で有効なすべての チャネルをスキャンできます。また、他の地域で使用可能なチャネルも同様です。ローカル モードのアクセス ポイントは、これらのチャネルのノイズと干渉を監視するために、最大で 70 ミリ秒の間「オフチャネル」になります。 不正アクセス ポイント、不正クライアント、アドホック クライアント、干渉しているアクセス ポイントを検出するために、この間に収集されたパケットが解析されます。

（注） 音声トラフィックやその他の重要なトラフィックがある場合（過去100ミリ秒内）、アクセス ポイントはオフチャネル測定を延期できます。また、アクセス ポイントは、WLAN スキャン プライオリティの設定に基づいてオフチャネルの測定を延期します。

各アクセス ポイントがオフチャネルになるのはすべての時間のわずか 0.2% です。この動作はすべてのアクセス ポイントに分散されるので、隣接するアクセス ポイントが同時にスキャンを実行して、無線 LAN のパフォーマンスに悪影響を及ぼすことはありません。

送信電力の制御

デバイスは、リアルタイムのワイヤレス LAN 状況に基づいて、アクセスポイントの送信電力を動的に制御します。

伝送パワー コントロール（TPC）アルゴリズムによって、RF 環境での変化に応じて、アクセス ポイントの電力が増減します。多くの場合、TPC は干渉を低減させるため、アクセス ポイントの電力を下げようとします。しかし、アクセス ポイントで障害が発生したり、アクセス ポイントが無効になったりして、RF カバレッジに急激な変化が発生すると、TPC は周囲のアクセスポイントで電力を上げることもあります。この機能は、主にクライアントと関係があるカバレッジ ホールの検出とは異なります。TPC はアクセス ポイント間におけるチャネルの干渉を回避しながら、必要なカバレッジ レベルを達成するために、十分な RF 電力を提供します。TPCv1 を選択することをお勧めします。 TPCv2 オプションは廃止されます。TPCv1 では、チャネル認識モードを選択できます。5 GHz の場合はこのオプションを選択し、2.4 GHz の場合はオフのままにすることをお勧めします。

最小/最大送信電力の設定による TPC アルゴリズムの無効化

TPC アルゴリズムは、数多くのさまざまな RF 環境で RF 電力を分散させます。ただし、自動電力制御では、アーキテクチャの制限事項やサイトの制限事項のため、適切な RF 設計を実装できなかった一部のシナリオは解決できない可能性があります。たとえば、すべてのアクセスポイントを互いに近づけて中央の廊下に設置する必要があるが、建物の端までカバレッジが必要とされる場合などです。

このようなケースでは、最大および最小の送信電力制限を設定し、TPCの推奨を無効化することができます。最大および最小の TPC 電力設定は、RF ネットワークの RF プロファイルを通じてすべてのアクセス ポイントに適用されます。

[Maximum Power Level Assignment] および [Minimum Power Level Assignment] を設定するには、[Tx Power Control] ウィンドウのフィールドに、RRM で使用される最大および最小の送信電力を入力します。これらのパラメータの範囲は -10 ～ 30 dBm です。最小値を最大値よりも大きくしたり、最大値を最小値よりも小さくしたりすることはできません。

最大送信電力を設定すると、RRM では、コントローラに接続されているすべてのアクセスポイントはこの送信電力レベルを上回ることはできません（電力が RRM TPC またはカバレッジホールの検出のどちらで設定されるかは関係ありません）。たとえば、最大送信電力を 11 dBm に設定すると、アクセス ポイントを手動で設定しない限り、アクセス ポイントが 11 dBm を上回って伝送を行うことはありません。

チャネルの動的割り当て

同じチャネル上の2つの隣接するアクセスポイントによって、信号のコンテンションや信号の衝突が発生することがあります。衝突の場合、アクセス ポイントではデータが受信されません。この機能は問題になることがあります。たとえば、誰かがカフェで電子メールを読むことで、近隣の会社のアクセスポイントのパフォーマンスに影響が及ぶような場合です。これらがまったく別のネットワークであっても、チャネル1を使用してカフェにトラフィックが送信されることによって、同じチャネルを使用している会社の通信が妨害される可能性があります。Devicesはアクセス ポイント チャネル割り当てを動的に割り当てて、衝突を回避し、キャパシティとパフォーマンスを改善することができます。チャネルは、希少な RF リソースの浪費を防ぐために再利用されます。つまり、チャネル1はカフェから離れた別のアクセスポイントに割り当てられます。これは、チャネル1をまったく使用しない場合に比べてより効率的です。

deviceの動的チャネル割り当て（DCA）機能は、アクセス ポイント間における隣接するチャネルの干渉を最小限に抑える上でも役立ちます。たとえば、チャネル 1 とチャネル 2 など、802.11b/g 帯域でオーバーラップする 2 つのチャネルは、同時に 11 または 54 Mbps を使用できません。deviceは、チャネルを効果的に再割り当てすることによって、隣接するチャネルを分離します。

（注） 非オーバーラップ チャネル（1、6、11 など）だけを使用することをお勧めします。

（注） チャネルの変更時に、無線をシャットダウンする必要はありません。

deviceは、さまざまなリアルタイムの RF 特性を検証して、次のようにチャネルの割り当てを効率的に処理します。

- アクセスポイントの受信エネルギー：各アクセスポイントとその近隣のアクセスポイント間で測定された受信信号強度。チャネルを最適化して、ネットワーク キャパシティを最大にします。
- ノイズ：ノイズによって、クライアントおよびアクセスポイントの信号の品質が制限されます。ノイズが増加すると、有効なセル サイズが小さくなり、ユーザー エクスペリエンスが低下します。deviceでは、ノイズ源を避けるようにチャネルを最適化することで、システム キャパシティを維持しながらカバレッジを最適化できます。過剰なノイズのためにチャネルが使用できない場合は、そのチャネルを回避できます。
- 802.11 干渉：干渉とは、不正アクセスポイントや隣接するワイヤレスネットワークなど、ワイヤレス LAN に含まれない 802.11 トラフィックのことです。Lightweight アクセス ポイントは、常にすべてのチャネルをスキャンして干渉の原因を調べます。802.11 干渉の量が定義済みの設定可能なしきい値（デフォルトは 10 %）を超えると、アクセス ポイントからdeviceにアラートが送信されます。その場合、deviceでは、RRM アルゴリズムを使用してチャネルの割り当てを動的に調整することで、干渉がある状況でシステムパフォーマンスを向上させることができます。このような調整によって、隣接する Lightweight アクセス ポイントが同じチャネルに割り当てられることがありますが、この設定は、干渉している外部アクセス ポイントが原因で使用できないチャネルにアクセス ポイントを割り当てたままにしておくよりも効果的です。

  また、他のワイヤレス ネットワークがある場合、deviceは、他のネットワークを補足するようにチャネルの使用を変更します。たとえば、チャネル 6 に 1 つのネットワークがある場合、隣接する無線 LAN はチャネル 1 または 11 に割り当てられます。この調整によって、周波数の共有が制限され、ネットワークのキャパシティが増加します。チャネルにキャパシティがほとんど残っていない場合、deviceはそのチャネルを回避できます。すべての非オーバーラップ チャネルが使用される非常に大規模な展開では、deviceでも最適な処理が行われますが、期待値を設定する際に RF 密度を考慮する必要があります。
- 負荷および利用率：利用率の監視が有効な場合、たとえば、ロビーとエンジニアリングエリアを比較して、一部のアクセスポイントが他のアクセスポイントよりも多くのトラフィックを伝送するように展開されていることを、キャパシティの計算で考慮できます。deviceは、パフォーマンスが最も低いアクセスポイントを改善するようにチャネルを割り当てることができます。チャネル構造を変更する際には、負荷を考慮して、現在ワイヤレス LAN に存在するクライアントへの影響を最小限に抑えるようにします。このメトリックによって、すべてのアクセスポイントの送信パケットおよび受信パケットの数が追跡されて、アクセス ポイントのビジー状態が測定されます。新しいクライアントは過負荷のアクセスポイントを回避し、別のアクセス ポイントにアソシエートします。*Load and utilization* パラメータはデフォルトでは無効になっています。

deviceは、このRF特性情報をRRMアルゴリズムとともに使用して、システム全体にわたる判断を行います。相反する要求の解決にあたっては、軟判定メトリックを使用して、ネットワーク干渉を最小限に抑えるための最善の方法が選択されます。最終的には、3次元空間における最適なチャネル設定が実現します。この場合、上下のフロアにあるアクセスポイントが全体的な無線LAN設定において主要な役割を果たします。

（注） 動的周波数選択（DFS）が有効なAP環境では、DCAチャネルでUNII2チャネルオプションを有効にして、デュアル5 GHz無線で100 MHzの分離を許可していることを確認します。

RRMスタートアップ モードは、次のような状況で起動されます

- シングルdevice環境では、deviceをアップグレードしてリブートすると、RRMスタートアップ モードが起動します。
- マルチdevice環境では、RRMスタートアップ モードは、RFグループ リーダーが選定されてから起動されます。
- RRMスタートアップ モードはCLIからトリガーできます。

RRMスタートアップ モードは、100分間（10分間隔で10回繰り返し）実行されます。RRMスタートアップ モードの持続時間は、DCA間隔、感度、およびネットワーク サイズとは関係ありません。スタートアップ モードは、定常状態のチャネル計画に収束するための高感度な（環境に対するチャネルを容易かつ敏感にする）10回のDCAの実行で構成されます。スタートアップ モードが終了した後、DCAは指定した間隔と感度で実行を継続します。

（注） DCAアルゴリズム間隔は1時間に設定されますが、DCAアルゴリズムは常に10分間隔（デフォルト）で実行されます。最初の10サイクルでは10分ごとにチャネル割り当てが行われ、チャネルの変更は、DCAアルゴリズムに従って10分ごとに行われます。その後、DCAアルゴリズムは設定された時間間隔に戻ります。DCAアルゴリズム間隔は定常状態に従うため、DCA間隔とアンカー時間の両方に共通です。

（注） RFグループ メンバーで動的チャネル割り当て（DCA）/伝送パワーコントロール（TPC）がオフになっていて、RFグループ リーダーが自動に設定されている場合、メンバーのチャネルまたは送信パワーは、RFグループ リーダーで実行されるアルゴリズムに従って変更されます。

カバレッジ ホールの検出と修正

RRMカバレッジ ホール検出アルゴリズムは、堅牢な無線パフォーマンスに必要なレベルに達しない無線LANの無線カバレッジの領域を検出することができます。この機能によって、Lightweightアクセス ポイントを追加（または再配置）する必要があるというアラートが生成されます。

RRM 設定で指定されたレベルを下回るしきい値レベル（RSSI、失敗したクライアントの数、失敗したパケットの割合、および失敗したパケットの数）で Lightweight アクセス ポイント上のクライアントが検出されると、アクセス ポイントからdeviceに「カバレッジ ホール」アラートが送信されます。このアラートは、ローミング先の有効なアクセスポイントがないまま、クライアントで劣悪な信号カバレッジが発生し続けるエリアが存在することを示します。device では、修正可能なカバレッジ ホールと不可能なカバレッジ ホールが識別されます。修正可能なカバレッジホールの場合、deviceでは、その特定のアクセスポイントの送信電力レベルを上げることによってカバレッジホールが解消されます。送信電力を増加させることが不可能なクライアントや、電力レベルが静的に設定されているクライアントによって生じたカバレッジホールがdeviceによって解消されることはありません。ダウンストリームの送信電力を増加させても、ネットワーク内の干渉を増加させる可能性があるからです。

無線リソース管理の制約事項

- AP の最大数をすでに保持している RF グループに AP が join しようとすると、デバイスはアプリケーションを拒否し、エラーをスローします。

RRM の設定方法

ネイバー探索タイプの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ap dot11 {24ghz | 5ghz} rrm ndp-type {protected | transparent}**
	例：
	`デバイス(config)#ap dot11 24ghz rrm ndp-type protected`
	`デバイス(config)#ap dot11 24ghz rrm ndp-type transparent`
		ネイバー探索タイプを設定します。デフォルトでは、モードは「transparent」に設定されます。
		• [protected]：ネイバー探索タイプを「protected」に設定します。パケットが暗号化されます。
		• [transparent]：ネイバー探索タイプを「transparent」に設定します。パケットはそのまま送信されます。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

送信電力制御の設定

送信電力制御のしきい値の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11** {**24ghz** | **5ghz**} **rrm tpc-threshold** *threshold_value* 例： `デバイス(config)#ap dot11 24ghz rrm tpc-threshold -60`	自動電力割り当てのために RRM が使用する送信電力制御のしきい値を設定します。範囲は -80 ～ -50 です。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

送信電力レベルの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 {24ghz | 5ghz} rrm txpower**{*trans_power_level* | **auto** | **max** | **min** | **once**} 例：	802.11 の送信電力レベルを設定します。 • [trans_power_level]：送信電力レベルを設定します。

	コマンドまたはアクション	目的
	`Device(config)#ap dot11 24ghz rrm txpower auto`	• [auto]：自動 RF をイネーブルにします。 • [max]：最大自動 RF 送信電力を設定します。 • [min]：最小自動RF送信電力を設定します。 • [once]：自動 RF を一度だけイネーブルにします。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

802.11 RRM パラメータの設定

高度な 802.11 チャネル割り当てパラメータの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event sensitivity** {**high** | **low** | **medium**} 例： `デバイス(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high`	CleanAir のイベント駆動型 RRM パラメータを設定します。 • [High]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最高に指定します。 • [Low]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最低に指定します。 • [Medium]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を中間に指定します。

	コマンドまたはアクション	目的

ステップ 3	**ap dot11** {**24ghz** | **5ghz**} **rrm channel dca** { | **anchor-time** | **global** {**auto** | **once**} | **interval** | **min-metric** | **sensitivity** {**high** | **low** | **medium**}}
	例：
	デバイス(config)#**ap dot11 24ghz rrm channel**
	dca interval 2
		802.11 帯域の動的チャネル割り当て（DCA）アルゴリズム パラメータを設定します。
		• ：DCA リストに追加するチャネル番号を入力します。
		• [anchor-time]：DCA のアンカー時間を設定します。範囲は 0 ～ 23 時間です。
		• [global]：すべての 802.11 Cisco AP の DCA モードを設定します。
		  • [auto]：自動 RF をイネーブルにします。
		  • [once]：自動 RF を一度だけイネーブルにします。
		• [interval]：DCA のインターバル値を設定します。値は 1、2、3、4、6、8、12、24 時間です。デフォルト値 0 は 10 分を意味します。
		• [min-metric]：DCA の最小 RSSI エネルギーメトリックを設定します。範囲は -100 ～ -60 です。
		• [sensitivity]：環境の変化に対する DCA 感度レベルを設定します。
		  • [high]：最高の感度を指定します。
		  • [low]：最低の感度を指定します。
		  • [medium]：中間の感度を指定します。

ステップ 4	**ap dot11 5ghz rrm channel dca chan-width** {**20** | **40** | **80**} 例： デバイス(config)#**ap dot11 5ghz rrm channel**	5 GHz 帯域のすべての 802.11 無線に対する DCA チャネル幅を設定します。チャネル幅を [20 MHz]、[40 MHz]、[80 MHz]、または [Best] に設定します。チャネル幅のデフォルト値は 20 MHz です。[Best] のデフォルト値は 80 MHz です。

	コマンドまたはアクション	目的
	dca chan-width best	制約を設定する場合は、事前にチャネル帯域幅を [Best] に設定します。
ステップ 5	**ap dot11** {**24ghz** | **5ghz**} **rrm channel device** 例： デバイス(config)#**ap dot11 24ghz rrm channel device**	802.11 チャネル割り当てで、非 Wi-Fi デバイスの継続的な回避を設定します。
ステップ 6	**ap dot11** {**24ghz** | **5ghz**} **rrm channel foreign** 例： デバイス(config)#**ap dot11 24ghz rrm channel foreign**	チャネル割り当てで、外部 AP の 802.11 干渉の回避を設定します。
ステップ 7	**ap dot11** {**24ghz** | **5ghz**} **rrm channel load** 例： デバイス(config)#**ap dot11 24ghz rrm channel load**	チャネル割り当てで、Cisco AP の 802.11 負荷の回避を設定します。
ステップ 8	**ap dot11** {**24ghz** | **5ghz**} **rrm channel noise** 例： デバイス(config)#**ap dot11 24ghz rrm channel noise**	チャネル割り当てで、802.11 ノイズの回避を設定します。
ステップ 9	**end** 例： Device(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 カバレッジ ホール検出の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： Device# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**ap dot11 {24ghz | 5ghz} rrm coverage data**{**fail-percentage | packet-count | rssi-threshold**} 例： デバイス**(config)#ap dot11 24ghz rrm coverage** **data fail-percentage 60**	データ パケットの 802.11 カバレッジ ホール検出を設定します。 • [fail-percentage]：アップリンクデータパケットの 802.11 カバレッジ失敗率のしきい値を、1 ～ 100% の範囲で設定します。 • [packet-count]：アップリンクデータパケットの 802.11 カバレッジ最小失敗数のしきい値を、1 ～ 255 の範囲で設定します。 • [rssi-threshold]：データパケットの 802.11 最小受信カバレッジレベルを、-90 ～ -60 dBm の範囲で設定します。
ステップ 3	**ap dot11 {24ghz | 5ghz} rrm coverage exception global** 例外レベル 例： デバイス**(config)#ap dot11 24ghz rrm coverage** **exception global 50**	802.11 Cisco AP のカバレッジ例外レベルを、0 ～ 100 % の範囲で設定します。
ステップ 4	**ap dot11 {24ghz | 5ghz} rrm coverage level global** *cli_min* 例外レベル 例： デバイス**(config)#ap dot11 24ghz rrm coverage** **level global 10**	802.11 Cisco AP クライアントの最小例外を、1 ～ 75 の範囲で指定します。
ステップ 5	**ap dot11 {24ghz | 5ghz} rrm coverage voice**{**fail-percentage | packet-count | rssi-threshold**} 例： デバイス**(config)#ap dot11 24ghz rrm coverage** **voice packet-count 10**	音声パケットの 802.11 カバレッジ ホール検出を設定します。 • [fail-percentage]：アップリンク音声パケットの 802.11 カバレッジ失敗率のしきい値を、1 ～ 100% の範囲で設定します。 • [packet-count]：アップリンク音声パケットの 802.11 カバレッジ最小失敗数のしきい値を、1 ～ 255 の範囲で設定します。

	コマンドまたはアクション	目的
		• [rssi-threshold]：音声パケットの 802.11 最小受信カバレッジレベルを、-90 ～ -60 dBm の範囲で設定します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 イベント ロギングの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ap dot11 24ghz | 5ghz rrm logging {channel | coverage | foreign | load | noise | performance | txpower}**
	例：
	`デバイス(config)#ap dot11 24ghz rrm logging channel`
	`デバイス(config)#ap dot11 24ghz rrm logging coverage`
	`デバイス(config)#ap dot11 24ghz rrm logging foreign`
	`デバイス(config)#ap dot11 24ghz rrm logging load`
	`デバイス(config)#ap dot11 24ghz rrm logging noise`
	`デバイス(config)#ap dot11 24ghz rrm logging performance`
	`デバイス(config)#ap dot11 24ghz rrm logging txpower`
		各種パラメータに対するイベント ロギングを設定します。
		• [channel]：802.11 チャネル変更ロギング モードを設定します。
		• [coverage]：802.11 のカバレッジ プロファイル ロギング モードを設定します。
		• [foreign]：802.11 外部干渉プロファイル ロギング モードを設定します。
		• [load]：802.11 負荷プロファイル ロギング モードを設定します。
		• [noise]：802.11 ノイズ プロファイル ロギング モードを設定します。
		• [performance]：802.11 パフォーマンス プロファイル ロギング モードを設定します。
		• [txpower]：802.11 送信電力変更ロギング モードを設定します。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 統計情報の監視の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11 24ghz | 5ghz rrm monitor channel-list**{**all | country | dca**} 例： `デバイス(config)#ap dot11 24ghz rrm monitor channel-list all`	noise/interference/rogue などのパラメータに 802.11 監視チャネル リストを設定します。 • [all]：すべてのチャネルを監視します。 • [country]：設定された国コードで使用するチャネルを監視します。 • [dca]：動的なチャネル割り当てで使用されるチャネルを監視します。
ステップ 3	**ap dot11 24ghz | 5ghz rrm monitor coverage** *interval* 例： `デバイス(config)#ap dot11 24ghz rrm monitor coverage 600`	802.11 のカバレッジ測定間隔を、60 ～ 3600 秒の範囲で設定します。
ステップ 4	**ap dot11 24ghz | 5ghz rrm monitor load** *interval* 例： `デバイス(config)#ap dot11 24ghz rrm monitor load 180`	802.11 負荷測定間隔を、60 ～ 3600 秒の範囲で設定します。
ステップ 5	**ap dot11 24ghz | 5ghz rrm monitor noise** *interval* 例：	802.11 のノイズ測定間隔（チャネル スキャン間隔）を、60 ～ 3600 秒の範囲で設定します。

	コマンドまたはアクション	目的
	デバイス(config)#**ap dot11 24ghz rrm monitor noise 360**	
ステップ 6	**ap dot11 24ghz | 5ghz rrm monitor signal** *interval* 例： デバイス(config)#**ap dot11 24ghz rrm monitor signal 480**	802.11 の信号測定間隔（ネイバーパケットの頻度）を、60 ～ 3600 秒の範囲で設定します。
ステップ 7	**end** 例： Device(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 パフォーマンス プロファイルの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dot11** {**24ghz** | **5ghz**} **rrm profile clients** *cli_threshold_value* 例： Device(config)#**ap dot11 24ghz rrm profile clients 20**	802.11 Cisco AP クライアント数のしきい値を、1 ～ 75 の範囲で設定します。
ステップ 3	**ap dot11** {**24ghz** | **5ghz**}**rrm profile foreign** *int_threshold_value* 例： Device(config)#**ap dot11 24ghz rrm profile foreign 50**	802.11 外部干渉のしきい値を、0 ～ 100 % の範囲で設定します。
ステップ 4	**ap dot11** {**24ghz** | **5ghz**} **rrm profile noise** *for_noise_threshold_value* 例： Device(config)#**ap dot11 24ghz rrm profile noise -65**	802.11 外部ノイズのしきい値を、-127 ～ 0 dBm の範囲で設定します。

	コマンドまたはアクション	目的
ステップ 5	**ap dot11** {**24ghz** | **5ghz**} **rrm profile throughput** *throughput_threshold_value* 例： `Device(config)#ap dot11 24ghz rrm profile throughput 10000`	802.11 Cisco AP スループットのしきい値を、1000 ～ 10000000 バイト/秒の範囲で設定します。
ステップ 6	**ap dot11** {**24ghz** | **5ghz**} **rrm profile utilization** *rf_util_threshold_value* 例： `Device(config)#ap dot11 24ghz rrm profile utilization 75`	802.11 RF 使用率のしきい値を、0 ～ 100% の範囲で設定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

高度な 802.11 RRM の設定

チャネル割り当ての有効化（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel-update** 例： `デバイス# ap dot11 24ghz rrm channel-update`	シスコ アクセス ポイントごとに 802.11 チャネル選択の更新を有効にします。 （注） **ap dot11 {24ghz | 5ghz} rrm channel-update** を有効にすると、DCA アルゴリズムのチャネル割り当てに対してトークンが割り当てられます。

DCA 動作の再開

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap dot11** {**24ghz** | **5ghz**} **rrm dca restart** 例： `デバイス# ap dot11 24ghz rrm dca restart`	802.11 無線の DCA サイクルを再開します。

電力割り当てパラメータの更新（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap dot11** {**24ghz** | **5ghz**} **rrm txpower update** 例： `デバイス# ap dot11 24ghz rrm txpower update`	各シスコ アクセス ポイントの 802.11 送信電力を更新します。

RF グループ内の不正アクセス ポイント検出の設定

RF グループ内の不正アクセス ポイント検出の設定（CLI）

始める前に

RF グループ内の各組み込みコントローラに同じ RF グループ名が設定されていることを確認します。

（注） この名前は、すべてのビーコン フレーム内の認証 IE を確認するために使用されます。組み込みコントローラに異なる名前が設定されている場合は、誤アラームが生成されます。

手順

	コマンドまたはアクション	目的
ステップ 1	例： デバイス#	組み込みコントローラに接続されたすべてのアクセスポイントについて、次の手順を実行します。 • [monitor]：AP モードをモニターモードに設定します。 • [clear]：AP モードをサイトに基づいてローカルまたはリモートにリセットします。 • [sensor]：AP モードをセンサーモードに設定します。 • [sniffer]：AP モードをワイヤレススニファモードに設定します。
ステップ 2	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 3	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**wireless wps ap-authentication** 例： `デバイス (config)# wireless wps ap-authentication`	不正なアクセスポイントの検出をイネーブルにします。
ステップ 5	**wireless wps ap-authentication threshold** *value* 例： `デバイス (config)# wireless wps ap-authentication threshold 50`	不正アクセス ポイント アラームが生成されるタイミングを指定します。検出期間内にしきい値（無効な認証 IE を含むアクセス ポイント フレームの数を示します）に達した場合またはしきい値を超えた場合に、アラームが生成されます。

	コマンドまたはアクション	目的
		しきい値の有効範囲は 1 ～ 255 で、デフォルトのしきい値は1です。アラームの誤判定を防止するには、しきい値を高い値に設定してください。 （注） RF グループ内のすべての組み込みコントローラで、不正アクセスポイントの検出としきい値を有効にします。 （注） 不正アクセスポイントの検出が有効になっていない組み込みコントローラが RF グループ内にある場合、この機能が無効になっている組み込みコントローラ上のアクセスポイントは不正アクセスポイントとして報告されます。

RRM パラメータと RF グループ ステータスの監視

RRM パラメータの監視

表 *1:* 無線リソース管理を監視するためのコマンド

コマンド	説明
show ap dot11 24ghz channel	802.11b チャネル割り当ての設定および統計情報を表示します。
show ap dot11 24ghz coverage	802.11b カバレッジの設定と統計情報を表示します。
show ap dot11 24ghz group	802.11b グループ化の設定と統計情報を表示します。
show ap dot11 24ghz logging	802.11b イベント ロギングの設定と統計情報を表示します。
show ap dot11 24ghz monitor	802.11b モニタリングの設定および統計情報を表示します。
show ap dot11 24ghz profile	すべての Cisco AP の 802.11b プロファイル情報を表示します。
show ap dot11 24ghz summary	802.11b Cisco AP の設定と統計情報を表示します。
show ap dot11 24ghz txpower	802.11b 送信電力制御の設定と統計情報を表示します。

コマンド	説明
show ap dot11 5ghz channel	802.11a チャネル割り当ての設定および統計情報を表示します。
show ap dot11 5ghz coverage	802.11a カバレッジの設定と統計情報を表示します。
show ap dot11 5ghz group	802.11a グループ化の設定と統計情報を表示します。
show ap dot11 5ghz logging	802.11a イベント ロギングの設定と統計情報を表示します。
show ap dot11 5ghz monitor	802.11a モニターリングの設定および統計情報を表示します。
show ap dot11 5ghz profile	すべての Cisco AP の 802.11a プロファイル情報を表示します。
show ap dot11 5ghz summary	802.11a Cisco AP の設定と統計情報を表示します。
show ap dot11 5ghz txpower	802.11a 送信電力制御の設定と統計情報を表示します。

RF グループ ステータスの確認（CLI）

ここでは、RF グループ ステータスの新しいコマンドについて説明します。

次のコマンドを使用して、 の RF グループ ステータスを確認できます。

表 *2:* アグレッシブ ロード バランシング コマンドの確認

コマンド	目的
show ap dot11 5ghz group	802.11a RF ネットワークの RF グループ リーダーであるコントローラの名前が表示されます。
show ap dot11 24ghz group	802.11b/g RF ネットワークの RF グループ リーダーであるコントローラの名前が表示されます。

例：RF グループの設定

次に、RF グループ名を設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# wireless rf-network test1
デバイス(config)# ap dot11 24ghz shutdown
デバイス(config)# end
デバイス # show network profile 5
```

次に、RF グループ内の不正アクセス ポイントの検出を設定する例を示します。

```
デバイス#
```

```
デバイス# end
デバイス# configure terminal
デバイス(config)# wireless wps ap-authentication
デバイス(config)# wireless wps ap-authentication threshold 50
デバイス(config)# end
```

ED-RRM について

突発的干渉は、ネットワーク上に突然発生する干渉であり、おそらくは、あるチャネル、またはある範囲内のチャネルが完全に妨害を受けます。Cisco CleanAir のイベント駆動型 RRM 機能を使用すると、電波品質（AQ）に対してしきい値を設定できます。しきい値を超過した場合には、影響を受けたアクセス ポイントに対してチャネル変更がただちに行われます。ほとんどの RF 管理システムでは干渉を回避できますが、この情報がシステム全体に伝搬するには時間を要します。Cisco CleanAir では AQ 測定値を使用してスペクトラムを連続的に評価するため、対応策を 30 秒以内に実行します。たとえば、アクセス ポイントがビデオ カメラからの干渉を受けた場合は、そのカメラが動作し始めてから 30 秒以内にチャネル変更によってアクセス ポイントを回復させることができます。

Cisco ワイヤレス LAN コントローラでの ED-RRM の設定（CLI）

手順

ステップ 1 次のコマンドを入力して、Cisco CleanAir 対応のアクセス ポイントで非常に高いレベルの干渉が検出された場合に、イベント駆動型無線リソース管理（RRM）の実行がトリガーされるよう設定します。

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event** ：802.11 の Cisco Lightweight アクセス ポイントの CleanAir による RRM パラメータを設定します。

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event sensitivity** {**low** | **medium** | **high** | **custom**}：802.11 の Cisco Lightweight アクセス ポイントの CleanAir による RRM 感度を設定します。デフォルトの選択は、Medium です。

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event rogue-contribution**：不正な寄与を有効にします。

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event rogue-contribution duty-cycle** *thresholdvalue*：不正な寄与のしきい値を設定します。値の範囲は 1 ～ 99 で、デフォルトの値は 80 です。

ステップ 2 次のコマンドを入力して、変更を保存します。

write memory

ステップ 3 次のコマンドを入力して、802.11a/n/ac または 802.11b/g/n ネットワークに対する CleanAir の設定を確認します。

show ap dot11 {**24ghz** | **5ghz**} **cleanair config**

以下に類似した情報が表示されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。